

WHAT IS CLAIMED IS:

1 1. A system for performing security operations on network data, the system
2 comprising:
3 memory;
4 a data coprocessor configured to transfer data into and out of the memory;
5 a plurality of processors coupled to the memory and to the data
6 coprocessor, each processor being configured to perform, in parallel to one another,
7 security operations on a portion of the data; and
8 a plurality of security coprocessors coupled to the memory, each security
9 coprocessor being coupled to a respective one of the processors and configured to assist
10 the respective processor in performing security operations on the portion of the data.

1 2. The system of claim 1, wherein each of the plurality of processors
2 comprises:
3 logic configured to identify a security association related to the portion of
4 the data;
5 logic configured to filter the portion of the data based on the identified
6 security association;
7 logic configured to divide the portion of the data into fragments and to
8 reassemble the fragments into the portion; and
9 logic configured to identify a sequence associated with the portion of the
10 data.

1 3. The system of claim 1, wherein each security coprocessor comprises:
2 logic configured to obscure the portion of the data when the portion is
3 non-secure data;
4 logic configured to decipher the portion of the data when the portion is
5 secure data;

6 logic configured to determine an integrity of the portion of the data; and
7 logic configured to establish a security association related to the portion of
8 the data, wherein the security association includes information used to obscure and
9 decipher the portion and to determine the integrity of the portion.

1 4. The system of claim 1, comprising:
2 a search engine coprocessor coupled to the memory and to the plurality of
3 processors, the search engine coprocessor being configured to exchange control
4 information between at least one of the memory and external system memory and each of
5 the plurality of processors for use in performing security operations on the data.

1 5. The system of claim 4, comprising:
2 a memory coprocessor coupled to the plurality of processors, the memory,
3 and the external system memory, the memory coprocessor configured to determine a
4 status of the memory and the external system memory.

1 6. The system of claim 1, wherein each of the plurality of processors is
2 further configured to perform, in parallel to one another, quality-of-service (QoS)
3 operations on the portion of the data in coordination with performing the security
4 operations.

1 7. The system of claim 6, wherein each of the plurality of processors
2 comprises:
3 logic configured to identify an information flow associated with the data;
4 logic configured to determine a priority of the information flow; and
5 logic configured to manage the transfer of data into and out of the memory
6 based on the priority of the information flow associated with the data.

1 8. The system of claim 7, comprising at least one of:
2 an enqueue coprocessor coupled to the plurality of processors and to the
3 data coprocessor, the enqueue coprocessor configured to manage the information flow
4 associated with the data external to the system;
5 a policy coprocessor configured to assist the plurality of processors in
6 managing the transfer of the data into and out of the memory by enforcing policies of the
7 information flow associated with the data; and
8 a counter coprocessor configured to provide statistics related to the
9 transfer of the data into and out of the memory and the enforcing of policies of the
10 information flow.

1 9. The system of claim 1, wherein each of the plurality of processors is
2 configured to execute programmable instructions for performing the security operations
3 on the portion of the data from a plurality of independent instruction streams, and can
4 switch between instruction streams in a single clock cycle.

1 10. The system of claim 9, wherein each of the plurality of security processors
2 includes separate queues corresponding to each of the independent instruction streams.

1 11. The system of claim 1, wherein each of the plurality of processors
2 comprises:
3 logic configured to compress the portion of the data prior to performing
4 the security operations when the portion is non-secure data; and
5 logic configured to decompress the portion of the data after performing the
6 security operations when the portion is secure data.

1 12. The system of claim 11, wherein each security processor is configured to
2 assist the respective processor in compressing and decompressing the portion of the data.

1 13. A method for performing security operations on network data, the method
2 comprising:
3 transferring data into memory;
4 performing security operations on respective portions of the data in
5 parallel using a plurality of processors;
6 using a plurality of security coprocessors to assist in performing the
7 security operations on the respective portions of the data, each security coprocessor being
8 coupled to a respective one of the processors; and
9 transferring the operated-on portions of the data out of the memory.

1 14. The method of claim 13, wherein the security operations performed by
2 each of the processors comprise:
3 identifying a security association related to a portion of the data;
4 filtering the portion of the data based on the identified security
5 association;
6 dividing the portion of the data into fragments;
7 reassembling the fragments into the portion of data; and
8 identifying a sequence associated with the portion of the data.

1 15. The method of claim 13, wherein the security operations assisted by each
2 of the security coprocessors comprise:
3 obscuring a portion of the data when the portion is non-secure data;
4 deciphering the portion of the data when the portion is secure data;
5 determining an integrity of the portion of the data; and
6 establishing a security association related to the portion of the data,
7 wherein the security association includes information used in obscuring and deciphering
8 the portion and in determining the integrity of the portion.

1 16. The method of claim 13, comprising:
2 exchanging control information between at least one of the memory and
3 external system memory and each of the plurality of processors for use in performing
4 security operations on the data.

1 17. The method of claim 13, comprising:
2 performing quality-of-service (QoS) operations on the respective portions
3 of the data in parallel using the plurality of processors in coordination with performing
4 the security operations.

1 18. The method of claim 17, wherein the QoS operations performed by each
2 of the processors comprise:
3 identifying an information flow associated with the data;
4 determining a priority of the information flow; and
5 managing the transfer of data into and out of the memory based on the
6 priority of the information flow associated with the data.

1 19. The method of claim 18, comprising:
2 managing the information flow after transferring the operated-on portions
3 of the data associated with the information flow out of the memory;
4 enforcing policies of the information flow associated with the data; and
5 providing statistics related to the transfer of the data into and out of the
6 memory and the enforcing of policies of the information flow.

1 20. The method of claim 13, comprising:
2 compressing the respective portions of the data prior to performing the
3 security operations when the portions are non-secure data; and

4 decompressing the respective portions of the data after performing the
5 security operations when the portions are secure data.

1 21. The method of claim 13, comprising:
2 using each security processor to assist the respective processor in
3 compressing and decompressing the portions of the data.

1 22. A computer readable medium containing a computer program for
2 performing security operations on network data, wherein the computer program
3 comprises executable instructions for:
4 transferring data into memory;
5 performing security operations on respective portions of the data in
6 parallel using a plurality of processors;
7 using a plurality of security coprocessors to assist in performing the
8 security operations on the respective portions of the data, each security coprocessor being
9 coupled to a respective one of the processors; and
10 transferring the operated-on portions of the data out of the memory.

1 23. The computer readable medium of claim 22, wherein the instructions for
2 performing security operations on respective portions of the data in parallel using a
3 plurality of processors comprise executable instructions for:
4 identifying a security association related to a portion of the data;
5 filtering the portion of the data based on the identified security
6 association;
7 dividing the portion of the data into fragments;
8 reassembling the fragments into the portion of data; and
9 identifying a sequence associated with the portion of the data.

1 24. The computer readable medium of claim 22, wherein the instructions for
2 using a plurality of security coprocessors to assist in performing the security operations
3 comprise executable instructions for:

4 obscuring a portion of the data when the portion is non-secure data;
5 deciphering the portion of the data when the portion is secure data;
6 determining an integrity of the portion of the data; and
7 establishing a security association related to the portion of the data,
8 wherein the security association includes information used in obscuring and deciphering
9 the portion and in determining the integrity of the portion.

1 25. The computer readable medium of claim 22, wherein the computer
2 program comprises executable instructions for:

3 exchanging control information between at least one of the memory and
4 external system memory and each of the plurality of processors for use in performing
5 security operations on the data.

1 26. The computer readable medium of claim 22, wherein the computer
2 program comprises executable instructions for:

3 performing quality-of-service (QoS) operations on the respective portions
4 of the data in parallel using the plurality of processors in coordination with performing
5 the security operations.

1 27. The computer readable medium of claim 26, wherein the instructions for
2 performing QoS operations on the respective portions of the data in parallel using the
3 plurality of processors in coordination with performing the security operations comprise
4 executable instructions for:

5 identifying an information flow associated with the data;
6 determining a priority of the information flow; and

7 managing the transfer of data into and out of the memory based on the
8 priority of the information flow associated with the data.

1 28. The computer readable medium of claim 27, wherein the computer
2 program comprises executable instructions for:
3 managing the information flow after transferring the operated-on portions
4 of the data associated with the information flow out of the memory;
5 enforcing policies of the information flow associated with the data; and
6 providing statistics related to the transfer of the data into and out of the
7 memory and the enforcing of policies of the information flow.

1 29. The computer readable medium of claim 22, wherein the computer
2 program comprises executable instructions for:
3 compressing the respective portions of the data prior to performing the
4 security operations when the portions are non-secure data; and
5 decompressing the respective portions of the data after performing the
6 security operations when the portions are secure data.